IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	10/653,327	**Group Art Unit:**	2109
Applicant(s):	Chih-Wei CHEN	**Examiner:**	Anish Sikri
Filing Date:	September 2, 2003	**Docket No.:**	7196-125/10310641
Title: NETWORK-LINKED COMPUTER PLATFORM CONFIGURATION DATA ACCESS MANAGEMENT METHOD AND SYSTEM		**Confirmation No.**	2925

MAIL STOP: AMENDMENT
Commissioner for Patents
Post Office Box 1450
Alexandria, VA 22313-1450

REPLY UNDER 37 C.F.R. 1.111

Dear Sir:

In response to the Office Action of May 24, 2007, please amend the above-identified application as follows:

Amendments to the claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A network-linked computer platform configuration data access management method for use on a network-linked computer platform that is provided with at least one management function and linked to a network system linked to a number of system administration workstations, for the purpose of allowing a group of system administrators to browse the configuration data of each management function of the network-linked computer platform at the same time while allowing only one system administrator to modify the configuration data of the same management function at the same time;

the network-linked computer platform configuration data access management method comprising:

establishing a table data module, which is a data-only module used to store the current-access-status property of each management function of the network-linked computer platform;

in the event of any one of the system administration workstations issues a management function ~~access~~ modification request, ~~inquiring~~ querying the table data module to determine whether the management function being requested for modification is currently being accessed; if NO, generating ~~an access~~ a modification-permit message; ~~whereas~~ if YES, generating ~~an access~~ a modification-inhibit message;

in response to the ~~access~~ modification-permit message, performing an access-status registration procedure to set the current-access-status property of the requested management function to TRUE in the table data module; and then permitting the requesting workstation to gain access to and modify the configuration data of the requested management function; and

in response to the ~~access~~ modification-inhibit message, performing ~~an access~~ a modification-inhibiting procedure to inhibit the requesting workstation to modify the configuration data of the requested management function.

2. (Currently amended) The network-linked computer platform configuration data access management method of claim 1, further comprising:

a timing procedure, which is capable of being activated to count time for a preset timeout length promptly after the system administrator at the requesting workstation starts modifying the configuration data of the requested management function, and which is further capable of generating ~~an access~~ a modification-inhibit message at timeout to inhibit ~~access~~ modification to the configuration data of the requested management function.

3. (Original) The network-linked computer platform configuration data access management method of claim 1, wherein the management function configuration data includes authorized user profiles, hard disk settings, and system security settings.

4. (Original) The network-linked computer platform configuration data access management method of claim 1, wherein the access-inhibiting procedure allows the system administrator at the requesting workstation to view the contents of the configuration data of the requested management function but not to modify.

5. (Currently amended) A network-linked computer platform configuration data access management system for use with a network-linked computer platform that is provided with at least one management function and linked to a network system linked to a number of system administration workstations, for the purpose of allowing a group of system administrators to browse the configuration data of each management function of the network-linked computer platform at the same time while allowing only one system administrator to modify the configuration data of the same management function at the same time;

the network-linked computer platform configuration data access management system comprising:

a table data module, which is a data-only module used to store the current-access-status property of each management function of the network-linked computer platform;

a request responding module, which is capable of detecting whether any one of the system administration workstations has issued a management function ~~access~~ modification request; and if YES, capable of issuing an inquiry request message;

an inquiry module, which is capable of being activated in response to the inquiry request message from the request responding module to inquire the table data module whether the management function being requested for modification is currently being accessed; if NO, the inquiry module generating ~~an access~~ a modification-permit message; ~~whereas~~ if YES, the inquiry module issuing ~~an access~~ a modification-inhibit message;

an access-status registration module, which is capable of being activated in response to the ~~access~~ modification-permit message from the inquiry module to set the current-access-status property of the requested management function to TRUE; and

an access module, which is capable of being activated in response to the ~~access~~ modification-permit message from the inquiry module to allow the system administrator at the requesting workstation to gain access to and modify the configuration data of the requested management function, and capable of being activated in response to the ~~access~~ modification-inhibit message from the inquiry module to inhibit the system administrator at the requesting workstation to modify the configuration data of the management function.

6. (Currently amended) The network-linked computer platform configuration data access management system of claim 5, further comprising:

a timing module, which is capable of being activated to count time for a preset timeout length promptly after the system administrator at the requesting workstation starts modifying the configuration data of the requested management

function, and which is further capable of generating an access-inhibit message at timeout to inhibit ~~access~~ modification to the configuration data of the requested management function.

7. (Original) The network-linked computer platform configuration data access management system of claim 5, wherein the management function configuration data includes authorized user profiles, hard disk settings, and system security settings.

8. (Original) The network-linked computer platform configuration data access management system of claim 5, wherein the access module, when inhibited, allows the system administrator at the requesting workstation to view the contents of the configuration data of the requested management function but not to modify.

9. (New) The network-linked computer platform configuration data access management method of claim 1, wherein the management function includes a group of subset functions individually assigned to have their own current-access-status, allowing different system administrators to access the subset functions at the same time.

10. (New) The network-linked computer platform configuration data access management method of claim 9, wherein all of the subset functions individually are collectively assigned to have the same current-access-status property, such that if a certain subset function is currently being accessed and modified by a system administrator, then all the other subset functions will be inaccessible for modification by any other system administrators.

11. (New) The network-linked computer platform configuration data access management system of claim 5, wherein the management function includes a group of subset functions individually assigned to their own current-access-status, allowing different system administrators to access the subset functions at the same time.

12. (New) The network-linked computer platform configuration data access management system of claim 11, wherein all of the subset functions individually are collectively assigned to have the same current-access-status property, such that if a selected subset function is currently being accessed and modified by a system administrator, then all the other subset functions will be inaccessible for modification by any other system administrators.

REMARKS

In the Official Action, claims 1 – 8 have been rejected as being unpatentable over HASAN et al. in view of STILL. Applicant respectfully traverses.

Claims 1, 2, 5 and 6 have been amended to replace the wording "management function access request," "access-inhibit message," "access-permit message," and "access inhibiting procedure" with "management function modification request," "modification-inhibit message" "modification-permit message," and "modification inhibiting procedure respectively. Support for the amendments is found in the specification, *inter alia* at, page 5, line 21 to page 6, line 11, page 6, lines 18-21, and page 8, lines 3-4 and 9-10.

New claims 9-12 are being submitted without adding prohibited new matter. Support for the new claims is disclosed, *inter alia,* at page 5, line 21 to page 6, line 11 of the specification.

It can be seen from the specification, the current-access-status property stored in the table data module is modified according to the management function modification request received by the system. In one embodiment, when a system administrator plans to modify configuration data of a management function, the current-access-status property stored in the table data module is changed from "FALSE" to "TRUE." Therefore, the configuration data of the same management function of the network-linked computer platform is modified by only one system administrator, so as to prevent conflict of configuration data in the network-linked computer platform that would otherwise cause abnormal operation or even a system crash.

The Examiner asserts that Hasan et al. (USPN 7,082,464) disclose, in column 16, lines 38-54, technical features that "in the event of any one of the

system administration workstations issues a management function access request, inquiring the table data module whether the management function being requested for modification is currently being accessed." However, Hasan et al., disclose in column 16, lines 38-54 that "[T]he administration model allows multiple administrators of any type to concurrently manage the system with each type of administrator limited to their scope. The access may be further limited by any concurrency controls that may be in effect in order to prevent conflicts that corrupt the management database. Access controls may be assigned to particular administrators. There are many access control schemes however there are some basic concepts that apply to establishing any access control scheme for administrators in the virtualized network management system. The access control scheme will specify whether the administrator has no access, read access only, or read and write access to any specific part of the management database within the scope of a particular administrator. Write access means that the administrator can make changes to the specified part of the database." From the above, it is clear that Hasan et al. only disclose that access control schemes comprise "no access," "read access only" and "read and write access."

Further, Hasan et al. disclose in column 16, lines 55-64 that "[I]f a specific part of the management database is available in scope to a data center or subscriber administrator, the access controls granted to either the data center or subscriber administrator should be determined by agreement made between subscriber and data center when the subscriber had contracted with the data center. For example if the subscriber had granted the data center exclusive right to configure or modify the infrastructure services contracted for, then only the data center administrators will have write access to these services." From the above, it is clear that Hasan et al. only disclose if the subscriber had granted the data center exclusive rights, only the data center administrators will have write access. Therefore, Hasan et al. do not teach or suggest that when a

management function modification request is received, the table data module is queried to identify whether the current-access-status property of the management function is FALSE and the configuration data of the requested management function is allowed to be modified.

The Examiner also cites Still (USPN 5,991,879) to reject the claims. However, Still discloses a method allowing the gradual deployment of a new security policy on a data processing system, to solve the problem that under the prior security system the access to the system objects and processes are seriously affected by valid users, which is different from that of the claims. Further, the function and setting of the "Flag" disclosed in Still's specification are different from those of "Status" of the present invention. The set and reset of the "Flag" is merely a record to identify the users who are allowed or not allowed to access system objects.

Therefore, for at least these reasons amended claims 1 and 5 are believed to be allowable over the proposed Hasan et al. and Still combination.

Dependent claims 2 - 4 and 6 - 9 are also believed to recite further patentable subject matter of the invention and therefore are also believed allowable over the prior art. As such, allowance of the dependent claims is deemed proper for at least the same reasons noted for the independent claims, in addition to reasons related to their own recitations. For example, with respect to claims 2 and 6, Still discloses in column 7, lines 46-66 that the security administrator changes the assist status over a period of time during which a requesting user will be considered by the tertiary state process for ongoing access to objects/processes. However, the objective of the claimed timing procedure is to reset the current-access-status property to FALSE after the preset timeout length, allowing each system administrator to modify the configuration data of a management function only for a limited period of time.

Therefore, Still does not teach or suggest the limitations of claims 2 and 6. As to claims 3 and 7, Still does not disclose hard disk settings related techniques. Accordingly, applicant respectfully requests reconsideration of the outstanding rejections and an indication of the allowability of all of the claims in the present application.

The above amendments have been presented merely for the purpose of clarification, and not to overcome the applied prior art. Accordingly, no estoppel is deemed to result from any of the present amendments.

The Director is authorized to charge any additional fee(s) or any underpayment of fee(s), or to credit any overpayments to Deposit Account **50-0337**. Please ensure that Attorney Docket No. **7196-125/10310641** is referred to when charging any payments or credits for this case.

Respectfully submitted,

Dated: August 15, 2007

By _____

Alan M. Lenkin

Reg. No. 40,063

Customer No. 000167
Fulbright & Jaworski L.L.P.
555 South Flower Street
Forty-First Floor
Los Angeles, CA 90071
Phone: (213) 892-9237
Fax: (213) 892-9494
E-mail: alenkin@fulbright.com